版 权 声 明

Tenda®是深圳市吉祥腾达科技有限公司注册商标。文中提及到的其它商标或商品名称均是他们所属公司的商标或注册商标。本产品的所有部分，包括配件和软件，其版权属深圳市吉祥腾达科技有限公司所有，在未经过深圳市吉祥腾达科技有限公司许可的情况下，不得任意拷贝、抄袭、仿制或翻译成其它语言。

本手册中的所有图片和产品规格参数仅供参考，随着软件或硬件的升级会略有差异，如有变更，恕不另行通知，如需了解更多产品信息，请浏览我们公司网站：

http://www.tenda.com.cn。

目　　录

第一章 简 介 3
1.1 功 能 3
1.2 包装内清单 4

第二章 硬件安装 5
2.1 前面板 5
2.2 后面板 5
2.3 安装环境 5
2.4 硬件安装步骤 6

第三章 连接到宽带路由器 7
3.1 建立局域网（LAN）连接 7
3.2 建立广域网（WAN）连接 7

第四章 配置路由器 8
4.1 建立正确的网络设置 8
4.2 ISP配置 8
4.2.1 快速设置 9
4.2.1.1 PPPOE拨号上网（ADSL） 9
4.2.1.2 动态IP 9
4.2.1.3 静态IP 10
4.3 配置说明 11
4.3.1 启动和登录 11
4.3.2 运行状态 12
4.3.3 基本设置 12
4.3.3.1 LAN口设置 13
4.3.3.2 WAN口设置 13
4.3.3.3 MAC地址克隆 14
4.3.3.4 域名服务器 14
4.3.3.5 路由器访问限制 15
4.3.4 DHCP服务器 15
4.3.4.1 DHCP服务器设置 15
4.3.4.2 DHCP客户端列表 16
4.3.5 高级设置 17
4.3.5.1 流量统计 17

4.3.5.2 端口监控 18
4.3.5.3 VLAN设置 18
3.3.5.4 带宽控制 19
4.3.5.5 LAN口IP控制 19
4.3.5.6 IP-MAC绑定 20
4.3.6 虚拟服务器 21
4.3.6.1 虚拟服务器 21
4.3.6.2 UPnP设置 22
4.3.6.3 DMZ主机 23
4.3.7 安全设置 23
4.3.7.1 客户端过滤 24
4.3.7.2 URL过滤 25
4.3.7.3 MAC地址过滤 26
4.3.7.4 防网络攻击 27
4.3.7.5 远端WEB管理 28
4.3.7.6 特殊应用过滤 28
4.3.8 路由设置 29
4.3.8.1 路由表 29
4.3.8.2 静态路由 29
4.3.9 系统工具 30
4.3.9.1 时间设置 30
4.3.9.2 动态DNS 30
4.3.9.3 备份设置 31
4.3.9.4 软件升级 32
4.3.9.5 恢复出厂设置 32
4.3.9.6 重启路由器 33
4.3.9.7 修改登录口令 33
4.3.9.8 系统日志 33
4.3.10 退出登录 34

附录一 在线技术支持简介 35

附录二 TCP/IP地址设置方法（以WinXP为例） 37

附录三：常用命令介绍 40

第一章 简 介

感谢您购买本公司 TEI480/480T/490T/4000 网吧/企业路由器。TEI480/480T/490T/4000 是腾达公司面向网吧/社区/企业/学校而设计的新一代多功能宽带接入产品。采用全球信赖的高品质、高稳定性能的 Intel IXP 高端网络专用处理器，超高主频，采用六层 PCB 专业设计，充分保证了整机性能强劲、稳定可靠。双向转发速率 200Mbps，可支持 60,000 多个联机数，封包处理快速稳定。强大的防火墙，有效防止各种黑客攻击、ARP 攻击与欺骗、ARP 病毒等等。TEI480/480T/490T/4000 除了包含所有宽带路由器常见功能外，还提供了诸多功能：客户机实时流量查看、基于 IP 的带宽控制、单机连接数控制、IP 与 MAC 绑定、端口镜像、VLAN、UPnP、DDNS、VPN Pass-through、防火墙等高级功能。使用前请先仔细阅读本手册。

1.1 功 能

符合 IEEE 802.3、IEEE 802.3u、IEEE 802.3x 标准

支持 CSMA/CD, PPPoE, PPP, IP, ARP, DHCP, TCP, UDP, HTTP, FTP, DNS

提供 1 个 10/100M 自适应以太网（WAN）接口，可接 xDSL/以太网/Cable

提供 4 个 10/100M 自适应以太网（LAN）接口，与内部局域网连接

支持端口带宽控制、端口 VLAN 划分和端口镜像功能

支持流量统计功能，可以分析整个网络的资源使用状况

支持 VPN Pass－through

支持基于 IP 或基于端口的 QoS 设置，可限制单机带宽

支持 IP 与 MAC 地址绑定，有效防范 ARP 攻击

支持虚拟服务器、特殊应用程序、DMZ 主机和静态路由等功能

支持连接数设置，可限制单机连接数

内建防火墙，支持 IP 地址过滤、域名过滤、MAC 地址过滤

可防止 DoS 攻击、ARP 攻击，能自动隔离带病毒的电脑，确保网络正常使用

支持远程和 Web 管理，全中文配置界面，提供简易设置向导

1.2 包装内清单

- TEI480/480T/490T/4000 网吧/企业路由器一台
- 国标电源线一根
- 用户手册一本
- 保修卡一份
- 合格证一张
- L 型支架两个
- 快速安装指南一张
- 脚垫四个

第二章 硬件安装

2.1 前面板

1） Reset ：复位按钮。按住此按钮约 5 秒钟，路由器 SYS 系统状态灯将同时闪烁，此时松开复位按钮，路由器将恢复出厂设置并自动启动。

2） 指示灯：

指示灯	描 述	功 能
POWER	电源指示灯	供电正常，指示灯长亮
SYS	系统状态指示灯	闪烁表示系统正常 常亮或熄灭表示系统不正常
Link/Act	广域网和局域网状态指示灯	常亮表示相应端口已正常连接 闪烁表示相应端口正在进行数据传输
100M	广域网和局域网速率指示灯	100M 灯常亮表示相应端口位于 100M 工作模式 100M 灯不亮表示相应端口位于 10M 工作模式

3） WAN：广域网端口（RJ-45）或光纤接口。连接 x DSL 或以太网。

4） 局域网端口：4 个 RJ-45 接口。计算机或 HUB/交换机通过这些端口连接进入局域网。

2.2 后面板

电源：使用专用配置电源。

2.3 安装环境

● 安装环境要求：

➢ 将路由器水平放置，尽量使路由器远离发热器件。

- ➢ 不要将路由器置于太脏或潮湿的地方。
- ➢ 路由器勿用湿布擦拭。

- **路由器推荐使用环境：**
  - ➢ 温度：0℃-40℃
  - ➢ 湿度：5％-90％ＲＨ(非雾水)

2.4 硬件安装步骤

1) 建立局域网连接

将路由器 LAN 口和局域网中的 Hub 或交换机连接。您也可以将路由器 LAN 口直接和您的计算机网卡连接。

2) 建立广域网连接

将 x DSL 或以太网接入五类线和路由器 WAN 口相连，或使光纤和路由器光纤模块相连。

备注：TEI4000 提供一个光纤扩展槽，支持光纤接入。

⚠**注意：采用光纤接入时，必须使路由器处于断电的情况下，检查确认连接正确后，方可给路由器通电，否则可能会导致广域网络连接失败，为避免产品规格不匹配，请使用 TENDA TER870S 光纤模块。**

3) 连接电源

将电源连接好，路由器将自行启动。

第三章 连接到宽带路由器

3.1 建立局域网（LAN）连接

请使用标准网线连接您的计算机网卡到 TENDA 路由器的 LAN 端口，或者是连接您的交换机、集线器到 TENDA 路由器的 LAN 端口。

3.2 建立广域网（WAN）连接

请使用标准网线将 xDSL Modem/Cable Modem 连接到 TENDA 路由器的 WAN 端口。

第四章　配置路由器

在正确使用路由器之前，您需要对计算机进行合理的网络配置，以便和路由器进行正常的通信。

4.1 建立正确的网络设置

- 将计算机的 IP 地址改为自动获取或指定 IP 地址，而路由器出厂时已经默认配置了 IP 地址“192.168.0.1”，启动 IE 浏览器并在地址栏输入“192.168.0.1”系统会提示用户输入用户名和密码，如图。在该登录界面输入用户名和密码（用户名和密码的出厂值均为“admin”）。建议用户初次进入系统后更改管理员的用户名和密码。



4.2 ISP 配置

- 本路由器支持三种常用的接入方式（路由器的默认接入方式为动态 IP 接入）： PPPOE 拨号上网(ADSL)：采用 PPPOE 虚拟拨号来进行 Internet 连接。

  动态 IP：宽带网络或者有线通（例如：长城宽带）通过 DHCP 服务为用户分配 IP 地址。

静态 IP：以太网宽带接入方式，ISP（例如：聚友网络）提供的固定 IP 地址。

4.2.1 快速设置

单击管理员模式画面的“下一步”，进入接入方式选择画面。如图显示了最常用的三种上网方式，请根据您的需要进行选择：

设置向导

本路由器支持四种常用的上网方式，请您根据自身情况进行选择。

ADSL虚拟拨号（PPPoE）

以太网宽带，自动从网络服务商获取IP地址（动态IP）

以太网宽带，网络服务商提供的固定IP地址（静态IP）

下一步

4.2.1.1 PPPOE 拨号上网（ADSL）

如果您的上网方式为“ADSL 虚拟拨号”，只需要在“上网帐号”及“上网口令”中输入框中输入 ISP 服务商提供给您的帐号信息。

设置向导-ADSL

您申请ADSL虚拟拨号服务时，网络服务商将提供给您上网帐号及口令，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。

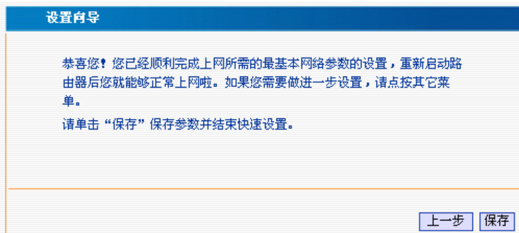
上网账号: szfcq179@163.gd

上网口令: ●●●●●●●●●●●●●●

上一步 下一步

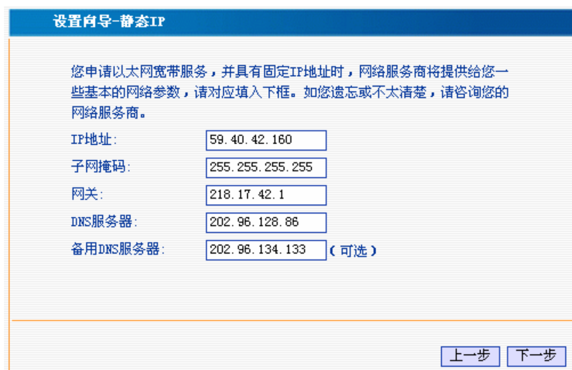
4.2.1.2 动态 IP

如果您的上网方式为“动态 IP”，通过此种接入，您可以从 ISP 服务商处动态获取到 IP 地址访问 Internet；不需其它设置，点击“下一步”保存即可。



4.2.1.3 静态 IP

如果您的上网方式为"静态 IP"，输入 ISP 提供给您的固定 IP 地址，子网掩码，网关地址以及 DNS 服务器、备用 DNS 服务器；点击"下一步"保存即可。



设置完成以后可以到"运行状态"中"WAN口状态"查看配置信息，通过点击"断开"按钮，可手动断开与Internet连接，点击"连接"按钮时，可恢复与Internet的连接。

WAN口状态

连接状态	已连接
WAN IP	59.40.6.77
子网掩码	255.255.255.255
网关	219.133.207.1
域名服务器	202.96.128.86
备用域名服务器	202.96.134.133
连接方式	PPPoE
连接时间	00:04:16
连接	断开

4.3 配置说明

4.3.1 启动和登录

- 在启动和登录成功以后，浏览器会显示管理员模式的画面。
- 在左侧菜单栏中，共有“运行状态”、“快速设置”、“基本设置”、“DHCP 服务器”、“高级设置”、“虚拟服务器”、“安全设置”、“路由设置”、“系统工具”、“退出登录”十个菜单。单击某个菜单项，您即可进行相应的功能设置。
- 下面将详细讲解各个菜单的功能。

4.3.2 运行状态



1) WAN 口状态

此处显示当前路由器连接状态、WAN IP、子网掩码、网关、域名服务器、备用域名服务器、连接方式。

2) LAN 口状态

此处显示当前路由器的 IP 地址、子网掩码和 DHCP 服务、NAT、防火墙的基本情况。

3） 信息

显示路由器当前运行时间、已连接客户端数，系统版本等信息

4.3.3 基本设置

在“基本设置”菜单下面，共有“LAN 口设置”、“WAN 口设置”、“MAC 地址克隆”和“域名服务器”“路由器访问限制”五个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.3.3.1 LAN 口设置

LAN口设置

本页设置LAN口的基本网络参数。

MAC 地址 00:02:B3:3C:16:95

IP地址 192.168.0.1

子网掩码 255.255.255.0

保 存 还 原 帮 助

- IP 地址：本路由器对局域网的 IP 地址。该 IP 地址的出厂设置为 192.168.0.1，您可以根据需要改变它。
- 子网掩码：本路由器对局域网中的子网掩码，可手动输入。

⚠**注意：如果您改变了本 IP 地址，您必须用新的 IP 地址才能登录路由器进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置为该 IP 地址才能正常上网。**

4.3.3.2 WAN 口设置

- 首先请您选择您的 WAN 口连接类型，即您的上网方式。本路由器默认的上网方式为“动态 IP”。

1） **动态 IP**：如果您的上网方式为动态 IP，即您可以自动从网络服务商（例如：长城宽带）获取 IP 地址。

2） **静态 IP**：如果您的上网方式为静态 IP，即您拥有网络服务商（例如：上海聚友网络）提供的固定 IP 地址。

3） **ADSL**：如果您的上网方式为 ADSL 虚拟拨号方式，在该页面您可以更改、设置以下项目：

- 上网账号：也就是您的上网账号，填入 ISP 为您指定的 ADSL 上网账号。
- 上网口令：填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。

- 服务名称：填入 ISP 为您提供的登陆服务名称。（可选）
- MTU：默认值为 1492，可根据您的需要进行修改。
- 自动连接：在开机和断线后自动进行连接。
- 手动连接：由用户手动进行连接。
- 按需连接，在有访问数据时自动进行连接。
- 定时连接，在指定的时段自动进行连接。

4.3.3.3 MAC 地址克隆

MAC地址克隆

本页设置路由器对广域网的MAC地址。

MAC 地址 00:02:B3:3C:16:96 恢复出厂MAC 克隆MAC地址

保 存 还 原 帮 助

- 将当前管理者使用计算机的 MAC 地址克隆成 WAN 口 MAC 地址（也可手动更改 MAC 地址）。

4.3.3.4 域名服务器

域名服务器

域名服务设置 □启用

域名服务器（DNS）地址 202.96.134.133

备用DNS地址 （可选） 202.96.128.68

保 存 还 原 帮 助

- 域名服务器(DNS)地址：填入 ISP 提供给您的 DNS 服务器，不清楚可以向 ISP 询问。
- 备用 DNS 地址（可选项）：如果 ISP 提供给您两个 DNS 服务器，则您可以把另一个 DNS 服务器的 IP 地址填于此处。

⚠注意：DNS 的主要作用是把我们输入的域名解析为 IP 地址。

4.3.3.5 路由器访问限制

为了增加路由器管理的安全性，您可以指定计算机的 IP 地址和更改路由器访问端口来进行 WEB 管理。

路由器WEB访问限制

为了使路由器本身设置不被其他非授权主机地址更改，可以启用该功能。

注意：设置WEB访问主机之后，其它地址的主机将不能登陆路由器WEB管理界面。更改端口之后，需重启路由器方可生效。

☐启用指定访问路由器WEB的主机和端口功能。

IP地址：0.0.0.0

端口 ：80

保 存 还 原 帮 助

⚠**注意：**设置指定 IP 地址之后，其它地址的主机将不能登陆路由器 WEB 界面。当修改访问路由器的端口时，**路由器需重新启动**。

例如：路由器的地址为 192.168.0.1，管理者的 IP 地址为 192.168.0.10，访问端口改为：8888，只有 IP 地址为 192.168.0.10 才能登陆路由器，则登陆管理页面的 IP 地址为：192.168.0.1:8888。

4.3.4 DHCP 服务器

- 在“DHCP 服务器”菜单下面，有“DHCP 服务器设置”和“DHCP 客户端列表”两个子项。下面将详细讲解各子项的功能。

4.3.4.1 DHCP 服务器设置

LAN端口DHCP服务器

DHCP服务器 ☑启用

IP池开始地址 192.168.0. 10

IP池结束地址 192.168.0. 100

过期时间 一天

保 存 还 原 帮 助

- 要使用 DHCP 服务器功能，您需要设置以下项目：
  - 启用 DHCP 服务器。
  - IP 池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。
  - IP 池结束地址：DHCP 服务器所自动分配的 IP 的结束地址。
  - 过期时间：每个客户端获得 IP 地址的使用时间。

注意：为了使用本路由器的 DHCP 服务器功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”。

4.3.4.2 DHCP 客户端列表

DHCP客户端列表

刷新

主机名	IP 地址	MAC 地址	租约时间	静态
td151	192.168.0.10	00:00:9A:06:02:26	1天 00:00:00	☐

静态分配

IP 地址 192.168.0.

MAC 地址 : : : : : 添加

保 存 还 原 帮 助

- 客户端列表列出了主机名、IP 地址、MAC 地址、租约时间及静态。
  - 主机名：客户端的主机名。
  - IP 地址：客户端申请到的 IP 地址。
  - MAC 地址：申请到该 IP 地址的计算机的 MAC 地址。
  - 租约时间：主机通过 DHCP 所获得的 IP 地址使用时间。
  - 静态分配：通过 MAC 地址绑定功能把 IP 地址分配给指定的客户端。
- 当路由器地址池分配尽后，将分配已过期的 IP 给新申请的用户。
- 填写“静态分配”栏，MAC 地址将与 IP 绑定，使计算机下次还是获得当前 IP 地址

注意：当局域网内的电脑 IP 地址设置为自动获取时，可在此给局域网内电脑分配 IP 地址。

4.3.5 高级设置

- 在“高级设置”菜单下面，有“流量统计 ”、“端口监控”、“VLAN 设置”和“端口带宽控制”“LAN 口 IP 控制”“IP-MAC 绑定”六个子项。单击某个子项，您即可进行相应的功能查看与设置。

4.3.5.1 流量统计

流量统计

本页统计了各个IP的数据流量和速率（↑代表发送，↓代表接收）。

按IP地址排序

		总流量				速率				
IP地址	MAC地址	↑包数	↑字节数	↓包数	↓字节数	↑速率	↓速率	连接数	操作	绑定
192.168.0.1	00:02:B3:3C:16:95	0	0	0	0	0	0	0	限制	导入
192.168.0.10	00:08:02:68:36:50	1905	149509	3193	4502853	0	0	2	限制	导入
192.168.0.11	00:E0:4C:FF:24:2B	297	27341	191	263802	0	0	0	限制	导入

刷 新　帮 助

本页统计了各个 IP 地址的数据流量、速率（↑代表发送，↓代表接收）、连接数、操作、绑定。

- IP 地址的数据流量、速率:显示该 IP 地址访问路由器和外网的数据量。
- 连接数：显示此 IP 地址建立的连接数。
- 操作：可以对此 IP 地址进行限制或解除。
- 绑定：把此 IP 地址与 MAC 地址导入进行绑定。但 IP-MAC 绑定中 ARP 绑定需启用。

⚠**注意：**如果未启用安全设置中的防网络攻击功能，会导致以上部分数据不准确。

4.3.5.2 端口监控

端口监控

本页设置端口监控的基本参数，端口监控功能可以将一个或多个被监控端口的数据包(发送或接收＋发送的数据包)转发到监控端口。

端口监控功能 ◉禁用 ○启用

监控端口：

被监控端口：

说明：

1、监控端口和被监控端口不能设置为同一个端口

2、当启用端口监控后，设置为被监控端口的所有数据都会复制一份到监控端口

保 存 帮 助

- 本页设置端口监控的基本参数，端口监控功能可以将一个或多个被监控端口的数据包(发送或接收＋发送的数据包)转发到监控端口。
  - 端口监控功能：开启或关闭端口监控功能。
  - 监控端口：用于采集被监控端口数据包的端口数据。
  - 被监控端口：任何输入、输出该端口的数据包都将被复制一份发给监控端口。

4.3.5.3 VLAN 设置

VLAN设置

本页设置VLAN功能的基本参数，本路由器支持基于端口的VLAN（Port base VLAN）功能，只有设置在同一个VLAN组的端口才能相互通讯。

VLAN组合模式： VLAN1

- 本页设置 VLAN 功能的基本参数，本路由器支持基于端口的 VLAN（Port

base VLAN）功能，只有设置在同一个 VLAN 组的端口才能相互通讯。

- VLAN 模式选择：根据注释选择需要的 VLAN 组合模式。

⚠注意：此功能可用于企事业单位部门数据的安全管理。

3.3.5.4 带宽控制

本页设置每个 LAN 口的网络传输带宽和连接数，我们可以根据局域网络结构来合理分配带宽资源，让网络资源可以得到充分利用。

带宽控制

本页设置每个LAN口的网络传输带宽，我们可以根据局域网络结构来合理分配带宽资源，让网络资源可以得到充分利用。

端口1	无限制
端口2	无限制
端口3	无限制
端口4	无限制

保 存 帮 助

- 您可以通过对相应的 LAN 口设置适当的带宽值来控制各端口的下载速率，从而达到合理分配带宽资源的目的。如果您不想对某 LAN 口的带宽进行限制，则可以将其设置为“无限制”。

4.3.5.5 LAN 口 IP 控制

本页可设置局域网内每个 IP 地址或 IP 地址段的实际传输带宽和对外的连接数，结合流量统计的功能可以有效的控制局域网内每台电脑的使用带宽，防止使用 BT、QQ 直播等下载工具恶意的抢占网络资源，可以均衡分配整个网络的流量。

- 上传速率和下载速率的范围为：8K、16、32K、64K、128K、256K、512K、1024、2048K、无限制。
- 连接数的范围为 0-999，“0”表示无限制。

LAN口IP控制

本页可设置局域网内每个IP地址或IP地址段的实际传输带宽,结合流量统计的功能可以有效的控制局域网内每台电脑的使用带宽,防止使用BT等下载工具恶意的抢占网络资源,可以均衡分配整个网络的流量。

☐ 使用下表中出现的规则，需选中该标志才能生效。

起始IP	终止IP	下载速率 KB/s	上传速率 KB/s	连接数限制	操作
	~	无限制	无限制		<<添加

保 存　帮 助

4.3.5.6 IP-MAC 绑定

本页设置单机的 MAC 地址和 IP 地址的匹配规则,防止其他非法 IP 地址和非法 MAC 地址接入网络，防止 ARP 欺骗。

- 全部导入：只是导入高级设置->流量统计中显示的 IP 和 MAC 地址，如网内需增加 IP 和 MAC 地址，需手动进行添加。
- 其它设置：增加单个条目、使能所有条目、删除所有条目、查找指定条目、保存。

ARP静态绑定

本栏设置单机的MAC地址和IP地址的匹配规则。

注：IP-MAC绑定自动导入操作请转**高级设置->流量统计**或者直接 全部导入

注意：该功能启用时，只有表中的IP地址才可以访问外网。

ARP绑定： ⦿不启用 ○启用

ID	局域网IP地址	MAC地址	绑定	配置

增加单个条目　使能所有条目　删除所有条目　查找指定条目

刷新　帮 助

⚠注意：如开启此功能，表中无任何 **IP** 地址和 **MAC** 地址，则网内计算机都无法连接网络，只有存在表中的 **IP** 和 **MAC** 地址才有权访问网络。

4.3.6 虚拟服务器

- 在“虚拟服务器”菜单下面，有“虚拟服务器 ”、“UPnP 设置”和“DMZ 主机” 三个子项。单击某个子项，您即可进行相应的功能查看与设置。

4.3.6.1 虚拟服务器

- 虚拟服务器被定义为一个服务端口，所有外部对此端口的访问将被转向到局域网提供服务器的计算机。

➢ 服务端口：LAN 端服务端口，即与 WAN 服务端口对接的内网服务端口。

➢ 内网 IP：输入需要开设虚拟服务的内部主机 IP。

➢ 协议：选择转发数据的协议类型 TCP/UDP/ALL。

➢ 启用：只有选中该项后本条目所设置的规则才能生效。

例如：您有一台 IP 为 192.168.0.2 的 WEB 服务器，端口 80，一台为 IP 为 192.168.0.3 的 FTP 服务器，端口为 21。那么您需要象下面这样虚拟服务器映射表。

ID	服务端口	内网IP	协议	启用	删除
1.	80	192.168.0.2	ALL	☑	☐
2.	21	192.168.0.3	ALL	☑	☐

⚠注意：如果设置了服务端口为 **80** 的虚拟服务器，则需要将“安全设置”菜单中“远端 **WEB** 管理”项设置为 **80** 以外的值，如 **8080**，否则会发生冲突，而导致虚拟服务器不起作用，此功能需要重启路由器才生效。

4.3.6.2 UPnP 设置

UPnP 设置

启用UPnP ☑

UPnP映射表

ID	远端主机	外部端口	内部主机	内部端口	协议	描述
1	58.60.252.74	2689	192.168.0.10	16808	UDP	MsnMsgr (192.168.0.10:16808) 2689 UDP

刷 新

保 存 还 原 帮 助

支持最新的 Universal Plug and Play (UPnP 通用即插即用网络协议)，此功能需要 Windows ME/Windows XP 以上的操作系统(注：系统需集成，安装 Directx 9.0 或更新版本)或支持 UPnP 的应用软件才能生效。例如：Windows ME/Windows XP 系统上安装了 MSN Messenger 在音频和视频通话时可以利用 UPNP 协议。

4.3.6.3 DMZ 主机

DMZ

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。
（注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。）

DMZ主机IP地址： 0.0.0.0 启用

保 存 还 原 帮 助

有些程序运行需要多个连接，比如：Internet 游戏、视频会议、Internet 电话等。由于路由器的防火墙的存在，这些程序无法在单纯的虚拟服务下工作。此时可以把该计算机设置成 DMZ 主机。

例如：将 IP 地址为 192.168.0.3 的做为 DMZ 主机。

DMZ主机IP地址： 192.168.0.3 启用

首先在 DMZ 主机 IP 地址输入需设为 DMZ 主机的局域网计算机的 IP 地址，然后点击“启用”完成 DMZ 主机的设置。

4.3.7 安全设置

- 在“安全设置”菜单下面，共有“客户端过滤”、“URL 过滤”、“MAC 地址过滤”、“防网络攻击”、“远端 WEB 管理”和“特殊应用过滤”六个子项。下面将详细讲解各子项的详细功能。

4.3.7.1 客户端过滤

客户端过滤

☐禁止下表中出现的数据包通过，允许其它数据包通过

ID	开始IP	结束IP	端口	类型	时间	启用	删除
1.			~	全部	0:00 ~ 0:00	☐	☐
2.			~	全部	0:00 ~ 0:00	☐	☐
3.			~	全部	0:00 ~ 0:00	☐	☐
4.			~	全部	0:00 ~ 0:00	☐	☐
5.			~	全部	0:00 ~ 0:00	☐	☐
6.			~	全部	0:00 ~ 0:00	☐	☐
7.			~	全部	0:00 ~ 0:00	☐	☐
8.			~	全部	0:00 ~ 0:00	☐	☐
9.			~	全部	0:00 ~ 0:00	☐	☐
10.			~	全部	0:00 ~ 0:00	☐	☐

保 存 还 原 帮 助

- 为了方便您对局域网中的计算机进行进一步管理，您可以通过客户端过滤功能来控制局域网中计算机对互联网的访问。

  设置客户端过滤的步骤如下：

  1) 打开“安全设置”主菜单，进入“客户端过滤”子菜单。
  2) 在“IP”栏内填入局域网中被控制的计算机的 IP 地址。
  3) 在“端口”添写欲控制的端口。
  4) 在“类型”下选择被控制的数据包所使用的协议。(“全部”包括 TCP/UDP)。
  5) 在“时间”栏内选择您希望本条规则生效的起始时间和终止时间。
  6) 选中“启用”，启用本条过滤规则。
  7) 单击“保存”完成设置。

例如：要禁止 IP 地址段 192.168.0.10～192.168.0.100 不能浏览网页，设置后如下图所示：

☑禁止下表中出现的数据包通过，允许其它数据包通过

ID	开始IP	结束IP	端口		类型	时间		启用	删除
1.	192.168.0.10	192.168.0.100	80	80	全部	全部	全部	☑	☐

4.3.7.2 URL 过滤

URL 过滤

☐启用URL过滤

索引	开始IP	结束IP	URL字符串	启用	删除
1.				☐	☐
2.				☐	☐
3.				☐	☐
4.				☐	☐
5.				☐	☐
6.				☐	☐
7.				☐	☐
8.				☐	☐
9.				☐	☐
10.				☐	☐

保 存　还 原　帮 助

- 为了方便您对局域网中的计算机所能访问的网站进行控制，您可以使用 URL 过滤功能来指定什么 IP 的客户端不能访问哪些网站。
- 设置 URL 过滤的步骤如下：
  1) 打开“安全设置”主菜单，进入“URL 过滤”子菜单。
  2) 选中“启用 URL 过滤”选项，启用 URL 过滤功能。
  3) 在 IP 栏内填入要控制的 IP 段。
  4) “URL 字符串”栏内填入被过滤的域名或域名的一部分，如果您在此处填入某一个字符串，被选中的计算机将不能访问所有域名中含有该字符串的网站。
  5) 选中“启用”，启用本条过滤规则，本规则仅对浏览器访问目标端

口为 80 的网站起作用。

6) 单击“保存”完成设置。

例如：要禁止 IP 地址段 192.168.0.10～192.168.0.100 不能访问 http://www.163.com，设置后如下图所示：

☑启用URL过滤

索引	开始IP	结束IP	URL字符串	启用	删除
1.	192.168.0.10	~ 192.168.0.100	www.163.com	☑	☐

4.3.7.3 MAC 地址过滤

MAC地址过滤

MAC地址过滤 ☐启用

仅允许/禁止列表中的MAC地址 ⦿仅禁止 ○仅允许

设置MAC地址

MAC 地址 注释 操作

<<添加 手动设置

保 存 还 原 帮 助

● 为了更好的对局域网中的计算机进行管理，您可以通过 MAC 地址过滤功能控制局域网中计算机对 Internet 的访问。

设置 MAC 地址过滤的步骤如下：

1) 打开“安全设置”主菜单，进入“MAC 地址过滤”子菜单。

2) 选中“启用”选项，启用 MAC 地址过滤功能。

3) 仅允许/禁止列表中的 MAC 地址，可选择仅允许（允许下列的 MAC 地址访问网络）或仅禁止（禁止下列的 MAC 地址访问网络）

4) 在“MAC 地址”栏内填入您希望控制的计算机的 MAC 地址，在“注释”栏内填入对该计算机的适当描述，您也可以在“操作”栏的下拉列表中选取已知主机的 MAC 地址，点击“添加”然后“确认”。完成设置。

4.3.7.4 防网络攻击

防网络攻击

通过本页的设置可以防止来自局域网络和广域网络的黑客及病毒攻击
注:只有启用了DoS攻击后其他项目才能正常使用.

防DoS攻击	☑	
忽略来自WAN口的Ping	☑	
过滤来自LAN口的Ping(防冲击波病毒攻击)	☐	
启用ICMP-FLOOD攻击过滤：	☑	
ICMP-FLOOD数据包阀值：(5～3600)	100	包/秒
启用UDP-FLOOD过滤：	☑	
UDP-FLOOD数据包阀值：(5～3600)	1500	包/秒
启用TCP-SYN-FLOOD攻击过滤：	☑	
TCP-SYN-FLOOD数据包阀值：(5～3600)	1000	包/秒

保 存 | 列 表 | 帮 助

- 在这里开启防止网络攻击的各项功能，保护您的网络安全。
  - 防 DoS 攻击：只有启动防 DoS 攻击后，其他功能才能使用。
  - 忽略来自 WAN 口的 Ping：忽略来自 WAN 口的 Ping。
  - 过滤来自 LAN 口的 Ping：启用可防冲击波病毒攻击。
  - 启用 ICMP-FLOOD 攻击过滤：启用后可防止 ICMP 洪水攻击。
  - 启用 UDP-FLOOD 过滤：启用后可防止 UDP 洪水攻击。
  - 启用 TCP-SYN-FLOOD 攻击过滤：启用后可防止 SYN 洪水攻击。

⚠注意：

1、 路由器一旦发现有电脑存在病毒或制造恶意攻击，自动将其限制，令其无法正常上网，您可以通过列表查看主机列表。

2、 当您确定列表中的电脑已经清楚病毒或删除了恶意攻击程序，可以将列表删除，恢复被禁止电脑的正常上网功能，如下表：

被禁止的主机列表:

ID	主机IP地址	主机MAC地址	操 作
1	192.168.0.2	00:E0:4C:00:00:75	☐

4.3.7.5 远端 WEB 管理

通常来讲，只有局域网内的用户才能管理路由器。假如有特殊需要，这个功能将使您能在远程管理路由器。

远端WEB管理

启用

IP 地址 0.0.0.0

端口 80

保 存 还 原 帮 助

注意：

路由器默认的远端 WEB 管理 IP 地址为 0.0.0.0，当启用时，广域网中所有计算机都能登录路由器执行远端 WEB 管理，如果您改变了默认的 IP 地址（例如改为 58.60.111.221），则广域网中只有具有指定 IP 地址（例如 58.60.111.221）的计算机才能登录到路由器管理页面。

4.3.7.6 特殊应用过滤

- 启用此功能可以禁用“MSN”与“QQ”上网聊天。

特殊应用程序过滤

禁用MSN

禁用QQ

保 存 还 原 帮 助

注意：

因为 QQ 使用多种登陆方式，并且不同版本的 QQ 频繁更换登陆服务器和登陆方式。如果此功能在您的环境中无法禁止 QQ 登陆，您可以咨询我们

的客户服务人员寻求解决方法。

4.3.8 路由设置

- 在“路由设置”菜单下面，共有“路由表”和“静态路由”两个子项。，下面将详细讲解各子项的详细功能。

4.3.8.1 路由表

系统路由表

目的IP	子网掩码	网关	metric	接口
0.0.0.0	0.0.0.0	218.17.42.1	0	ixe1
192.168.0.0	255.255.255.0	192.168.0.1	0	ixe0
58.60.252.74	255.255.255.255	58.60.252.74	0	ixe1

刷 新

- 本页显示路由器核心路由表的内容。

4.3.8.2 静态路由

静态路由表

目的网络IP	子网掩码	网关	操作
			<<添加

帮 助

- 本页设置路由器的静态路由功能，您可以指定静态路由规则。

➢ **目的网络 IP**：目的主机的 IP 地址或目的网络的 IP 地址。

➢ **子网掩码**：目的地址的子网掩码，一般为 255.255.255.0。

➢ **网关**：下一跳路由器入口的 IP 地址。

注意：

1、网关 **IP** 必须是与 **WAN** 或 **LAN** 口属于同一个网段。

2、目的 **IP** 地址如果是一台主机 **IP** 地址，子网掩码须为 **255.255.255.255**。

3、目的 **IP** 地址如果为 **IP** 网段，则须与子网掩码匹配。例如，如果目的

IP 为 10.0.0.0，子网掩码须为 255.0.0.0；如果目的 IP 为 10.1.2.0，子网掩码须为 255.255.255.0。

4.3.9 系统工具

- 在“系统工具”菜单下面，共有“时间设置”、“动态 DNS”、“备份设置”、“软件升级”、“恢复出厂设置”、“重启路由器”“修改登录口令”和“系统日志”八个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.3.9.1 时间设置

时间设置

本页设置路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的GMT时间。

注意：关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能（如防火墙）中的时间限定才能生效。

时区：

（GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北

（注意：仅在连上互联网后才能获取GMT时间。）

保 存 还 原 帮 助

- 您可以选择自己设置时区从互联网上获取标准的 GMT 时间。当连上互联网后才能获取 GMT 时间。

4.3.9.2 动态 DNS

DDNS服务

本路由器内建动态DNS客户端支持。

DDNS服务 启用 不启用

服务提供商 oray.net 注册去

用户名： 用户名

密码： ••

域名 (可选)

保 存 还 原 帮 助

- 您只须要在花生壳（Oray.net）注册您的域名，把您注册的用户名与密码填入其中，保存好，您就可以通过本路由的 DDNS 服务在外网用域名直接访问您在本地建立的服务器(例：在本地 192.168.0.111 主机上建立一个 WEB 服务器，在花生壳注册的用户名是：qp612，域名是：qp612.vicp.net，在虚拟服务中映射好端口，就可以直接在浏览器的地址栏中输入“http:// qp612.vicp.net”就可以访问您的 WEB 页了。

4.3.9.3 备份设置

备份/恢复设置

您可以备份/恢复路由器的当前设置

选择文件名: backup.bin

选择TFTP Server: 192.168.0.10

恢复 备份

- 在这里您可以备份当前或恢复以前的路由器设置。

备份/恢复设置步骤：

1. 登录我们公司的网站（www.tenda.com.cn），下载一个 TFTP Server 应用程序，将此程序放到一个固定的目录中并运行。
2. 单击“备份”便可以在 TFTP 应用程序的目录生成一个系统配置的备份文件。
3. 同样道理，我们只需要把需要上传的系统配置文件放置到 TFTP 的目录中，点击“恢复”，**重新启动路由器**后将可以恢复到以前的系统配置。

4.3.9.4 软件升级

软件升级

通过升级本路由器的软件，您将获得新的功能。

选择固件文件: upgrade.bin

选择TFTP Server: 192.168.0.10

当前系统版本: Ver 0.9.4.5a-Sep 27 2006 15:22:38

注意：升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级成功后，路由器将自动重启。升级过程约数分钟，请等候。

升 级　帮 助

通过升级本路由器的软件，您将获得更加稳定的路由器版本及增值的路由功能。请登陆我们公司的网站（www.tenda.com.cn）查看升级说明文档。

⚠**注意：升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级成功后，路由器将自动重启。最好更好的使用本路由器，升级完后请恢复出厂设置。**

4.3.9.5 恢复出厂设置

恢复出厂设置

单击此按钮将使路由器的所有设置恢复到出厂时的默认状态。

恢复出厂设置

帮 助

- “恢复出厂设置”按钮将使路由器的所有设置恢复到出厂时的默认状态。其中：
  - 默认的用户名为：admin
  - 默认的密码为：admin
  - 默认的 IP 地址为：192.168.0.1
  - 默认的子网掩码为：255.255.255.0
  - 恢复出厂设置后，路由器重新启动才能生效。

4.3.9.6 重启路由器



- “重启路由器”选项将使一些需要重新启动路由才能生效的设置生效。路由器在重启前，会自动断掉网络连接。

4.3.9.7 修改登录口令

修改登录口令

本页修改系统管理员的用户名及口令。

用户名 admin
原口令 ••••••
新口令 ••••••
确认新口令 ••••••

保 存 还 原 帮 助

- 本页修改系统管理员的用户名和口令。
- 请您首先输入新的用户名和原来的登陆口令，然后输入您希望使用的新的口令 ，如果您原来的用户口令输入无误的话，单击“保存”即可成功修改系统的用户名和口令。

⚠注意：出于安全考虑，我们强烈推荐您改变初始系统员用户名和密码。

4.3.9.8 系统日志

- 在系统日志里，您可以查看系统启动出现的各种情况，也可以查看有无网络攻击发生。
- 清除日志：清除系统日志。



4.3.10 退出登录

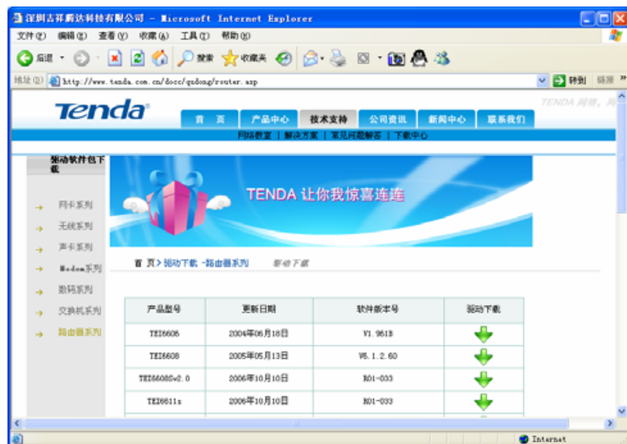
- 各项设置完成后请从“退出登录”安全的完全退出路由器的 WEB 管理页面。

附录一　在线技术支持简介

如果您在安装过程中遇到问题，请登录我们的网站 www.tenda.com.cn



技术支持的下载中心有最新的驱动程序和升级包下载：



还有常见问题解答：



当然，我们还有完善的售后服务电话为您提供技术支持：



附录二 TCP/IP 地址设置方法（以 WinXP 为例）

依次点击“开始—控制面板”，打开控制面板。（如图 1）。



图 1

单击“网络和 Internet 连接”，进入网络和 Internet 连接页面（如图 2）。



图 2

单击“网络连接”，进入网络连接页面（如图 3）。

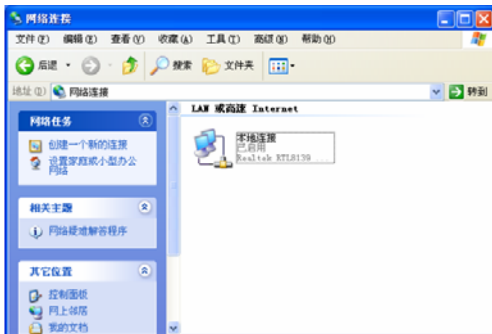


图 3

选择“本地连接”，点击鼠标右键，选择“属性”，弹出“本地连接 属性”对话框，在“此连接使用下列项目”中选择“Internet 协议 （TCP/IP）”，点击“属性”（如图 4）。

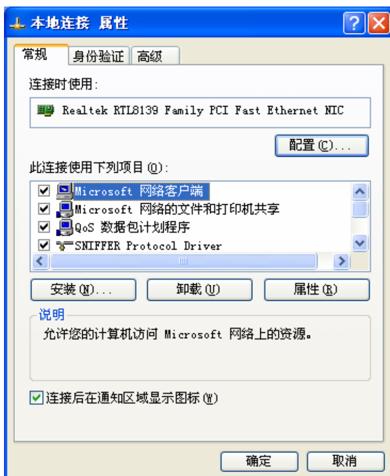


图 4

选择“使用下面的 IP 地址”，填写 IP 地址为：192.168.0.xxx.（xxx 为 2~254 中除了 1 的任意数值），子网掩码为 255.255.255.0（如图 5）。

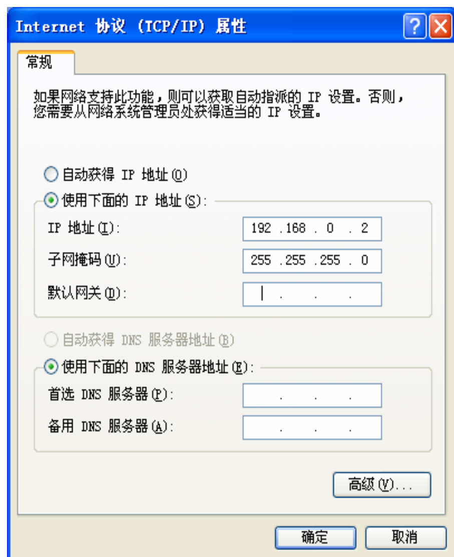


图 5

点击“确定”回到“本地连接 属性”对话框。

再点击“确定”退出设置界面。

在这一节中，我们介绍一下如何为您的个人计算机配置 TCP/IP 协议。

请您确认已经在您的计算机中成功安装了网卡，如果没有，请参阅网卡的用户手册，正确安装网卡硬件及驱动程序。

附录三：常用命令介绍

常用命令	命令说明
cmd	运行此命令可快速进入 Windows 的命令行模式（适用与 Windows2000 以上操作系统）
ipconfig	显示本机 IP 地址，如 ipconfig /all 查看
ping	这是 TCP / IP 协议中最有用的命令之一，它给另一个系统发送一系列的数据包，该系统本身又发回一个响应，这条实用程序对查找远程主机很有用，它返回的结果表示是否能到达主机，宿主机发送一个返回数据包需要多长时间。
netstat	能检验 IP 的当前连接状态，在断定您的基本级通信正在进行后，就要验证系统上的服务。这个服务包括检查正在收听输入的通信量或验证您正在创建一个与远程站点的会话，它可以很轻松地做到这一点。
tracert	Tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能同 Ping 类似，但它所获得的信息要比 Ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。
net stop	停止 Windows NT 网络服务，如：net stop dnscache
net send	向网络的其他用户、计算机或通信名发送消息。要接收消息必须运行信使服务。